IT Disaster Recovery and Business Resumption Planning Standards

Adopted by the Information Services Board (ISB) on May 28, 1992
Policy No: 501-S1 Also see: 500-P1, 502-G1
Supersedes No: N/A
Effective Date: July 1, 1993
Revision Date: April 2002 Definitions

Table of Contents

Introduction

All state agencies and educational institutions using or providing computing or voice, data, or video telecommunications services must prepare disaster recovery/business resumption plans. Included are:

- Agencies with their own computing or telecommunications facilities.
- Agencies that provide computer or telecommunications services to others.
- Agencies using computing or telecommunications services supplied by providers external to their organization.

Agency disaster recovery/business resumption plans shall provide all applicable information required by these standards.

Statutory Authority

The provisions of RCW 43.105.041 detail the powers and duties of the ISB, including the authority to develop statewide or interagency information services and technical policies, standards and procedures.

Scope

These standards apply to all executive and judicial branch agencies and educational institutions, as provided by law, that operate, manage, or use IT services or equipment to support critical state business functions.

Exemptions

None.

Standards

Each agency is responsible and accountable for its own disaster recovery/business resumption program. Agencies using external services shall coordinate their disaster recovery/business resumption plans with service providers.

The disaster recovery/business resumption plan is primarily for agency use. Agencies may adapt this standard to meet individual needs, but all applicable elements of the standard must be included in their plan. A disaster recovery/business resumption plan must contain enough information to enable agency management to assure the agency's ability to resume mission-critical computing and telecommunications services and operations. A disaster recovery/business resumption plan may contain references to another organization's disaster recovery/business resumption plan, or to an agency's internal policy, standards, or procedures manual. The State Auditor may audit agency disaster recovery/business resumption plans and test results for compliance with policy and standards.

Agencies shall review, update, and test their disaster recovery/business resumption plans annually, or more frequently if appropriate. Agencies must update their plans whenever agency computing or telecommunications environments undergo significant changes. Such changes may include: physical facility, computer hardware/software, telecommunications hardware/software, telecommunications networks, application systems, organization, or budget.

If an agency purchases IT services from another organization, the agency must make certain its disaster recovery/business resumption plan for those services fits with the service provider's plan. If two or more agencies participate in operating an information service facility, they must develop a joint disaster recovery/business resumption plan that meets their mutual needs.

Plan Contents

Overview

Describe the purpose and organization of the plan. Document state procedures for updating and distributing the plan. Describe the process for periodic (at least annual) testing of the plan.

Business Impact Analysis

Document the operational, legal, and financial impact from a disruption or disaster affecting any computer or telecommunication service area of the agency.

Risk, Threat, and Vulnerability Analysis

Document the threats that could debilitate computer or telecommunication service areas and cause business interruption; determine the probability of occurrence of each identified threat. Determine the vulnerabilities of service areas to potential threats. Estimate the loss potential of a service area, either by quantitative or qualitative means. Define the level or duration of service outage that constitutes a disaster or triggers the recovery plan.

Recovery Strategy

Document the general recovery strategy the agency will use in event of a disaster. There are different levels or degrees of disaster. Procedures should aim at coping with the worst case. Start with a narrative of the agency's strategy for managing the disaster situation. The recovery strategy is an overview of the recovery process that the organization will follow if affected by a disaster. The strategy should address:

1. Recovery requirements for critical business operations.
2. A description of provisions for off-site storage of critical data.
3. A description of the agency's alternative processing strategies and facilities such as:
    - Command centers.
    - Alternate business operations.
    - Alternate data processing.
    - Alternate data communications.
    - Alternate voice communications.
4. Procedures for obtaining resources during both the recovery phase and the restoration phase.

Emergency Response/Problem Escalation

Emergency response/problem escalation procedures prescribe how to respond to two kinds of situations:

1. **Disaster events**. Fires, floods, earthquakes, and bombings are examples of disaster events. They often take the form of unforeseen events that cause damage

or lengthy disruption or threaten to do so. One can often more readily recognize the situation is a disaster with these types of occurrences.

2. **Problems**. Disasters may evolve from problems that disrupt normal operations and then worsen or continue so long the disruption becomes critical. Examples: power "brownout," a computer virus, inclement weather, flu epidemic, sabotage, negligence, disk drive failure, local telephone service failure, or software failure.

Disaster recovery plans should address specific procedures for both situations. Emergency procedures direct the response to disaster events. Escalation procedures direct the response to problems. Both sets of procedures may result in the declaration of a disaster and activation of the recovery plan.

Emergency Response

Disaster recovery plans should document the emergency response actions the agency must take immediately to:

1. Protect the lives and safety of all personnel.
2. Gain immediate emergency help from fire, police, and hospitals.
3. Reduce outage duration or loss of IT services or assets.
4. Inform staff who are members of the agency disaster recovery/business resumption management team a serious loss or interruption in service has occurred.
5. Set up a focal point for coordinating the recovery program, sending out information, and assembling personnel.
6. If appropriate, establish contact with the Office of Emergency Management.

Problem Escalation

Disaster recovery plans must state the steps to follow for escalating unresolved problems to disaster status. The purpose of problem escalation procedures is to define the steps and time intervals leading up to the declaration of a disaster.

These procedures require use of a "contact tree", a list of individuals to be notified of the situation at specified time durations following the onset. The contact tree represents an ever-widening circle of management and key technical people. Such a procedure ensures key decision makers become aware of the situation in order to make more timely and informed decisions. As the situation becomes more pressing, the procedure must trigger calls to the disaster recovery/business resumption team, upper levels of management, clients, suppliers, and the public.

Plan Activation

First alert procedures:

Document general guidelines for initial notification of a potential disaster situation.

Disaster confirmation procedures:

- Document procedures to manage the initial assessment of a disaster or potential disaster situation.
- Document procedures and specify the personnel necessary to assess the damage and determine the level of severity of the incident.
- Document procedures for reporting findings to management.
- Document procedures for making initial emergency contacts.
- Document procedures for possible command center activation.
- Document recovery team notification procedures.
- Document procedures for declaring a disaster. Describe the decision support mechanism required to declare a disaster—versus a less severe interruption in processing capability.
- Document procedures for informing employees, the public, customers, and suppliers.

Recovery Operations

Recovery flow:

Outline or chart the sequence of steps to follow when a disaster situation has occurred or potentially may occur.

Recovery team organization:

1. Document staff and management responsibilities for putting the recovery plan into effect.
2. Identify an alternate for each team member.
3. Include team or individual assignments of responsibility by area of expertise such as:
   - Technical staff in the areas of systems software, telecommunications, and computer operations.
   - Program staff and management to aid in resolution of programmatic issues.
   - Business services to support such tasks as arranging for office space, supplies, equipment, and processing of emergency contracts.
4. Personnel and communications staff to issue information about special work assignments, conditions, or locations.

Recovery team plans:

1. Document the procedures required to achieve recovery rapidly. A portion of this documentation should consist of the process for recovering the critical data-processing activities. If appropriate, the latter should encompass transition to manual procedures and logistics of moving to an alternate facility.
2. Procedures for each team should, at a minimum, consist of:
   - Team charter.
   - Membership.

- Interfaces.
- Preparation requirements.
- Action procedures.
- Appendices.

Primary site restoration or relocation:
Document the procedures to use after the interim processing situation has stabilized. The intent is to provide a framework for restoring full processing capability at a permanent location.

Plan Validation/Testing

Document the disaster recovery/business resumption plan testing program. Specify necessary tests and assign responsibility for overseeing testing. Clearly state the purposes for conducting tests of the recovery plan. Include the policies and guidelines that will apply to testing of the recovery plan. Formulate a test schedule. For each test, specify the level of the test, the scope or areas to test, and the frequency or target date of the test. Include a brief report describing results achieved for each completed test. Agencies using external services shall plan, schedule, and conduct their disaster recovery/business resumption plan testing in cooperation with service providers.

Training

Specify the aims, training activities, schedule, and an administrator for agency disaster recovery/business resumption training. Describe regularly occurring training activities.

Plan Maintenance

Assign plan maintenance responsibility. Provide a schedule for regular, systematic review of the content of the disaster recovery/business resumption plan. Document the procedure used for making changes to the plan. Provide policies and procedures for distributing the disaster recovery/business resumption plan and updates to the plan. The disaster recovery/business resumption plan may contain sensitive information about the agency's business, communications, and computing operations. Policy and procedures for distribution of the plan should take this into account.

Plan Appendices

Agencies may attach a variety of appendices to the plan. The plan sections described above should contain static procedures. Appendices should contain information that needs continual updating.
Examples of content are:

- Emergency action notification information containing the names and phone numbers of management, staff, recovery team members, vendors, suppliers, service providers, and customers.
- Damage assessment or disaster classification forms intended to support the management decision process.
- Profiles of critical applications.
- Agency hardware, software, office space, and office furniture inventories.
- Voice and data communications network routing information necessary to provide interim processing capability.

Maintenance

Technological advances and changes in the business requirements of agencies will necessitate periodic revisions to policies, standards, and guidelines. The Department of Information Services is responsible for routine maintenance of these to keep them current. Major policy changes will require the approval of the ISB.